

# セキュリティガイドブック

TAKETIN MPが行っているセキュリティ対策のご説明及びお客様のご利用におけるセキュリティ上の注意点を

<b>はじめに</b>	<b>2</b>
<b>TAKETIN（タケチン）が機能として持つセキュリティ対策</b>	<b>3</b>
パスワードのハッシュ化	3
ログインIDとパスワードによるユーザー認証	3
管理者権限の管理（役割と権限）	3
管理画面を利用できるIPアドレスの制限	3
管理画面URLの変更	3
<b>サーバー運用・管理上のセキュリティ対策</b>	<b>4</b>
管理水準の高いデータセンター	4
RAID構成によるデータ保全	4
通信の安全性	4
ハードディスクの空き容量の監視	4
サーバーへのアクセス制限	4
<b>弊社におけるセキュリティ対策</b>	<b>5</b>
国際的なセキュリティ基準に則した運用体制	5
開発に関わる関係者とは機密保持契約	5
安心のバックアップ体制	5
<b>利用上のお願い</b>	<b>6</b>
ユーザーIDの、パスワードの漏洩防止	6
パスワードの定期的な変更	6
2段階認証の設定	6
データバックアップ	6
万が一に備えての保険加入もご検討ください	6

## はじめに

この度は、弊社「TAKETIN MP(タケチン マーケティング プラットフォーム)」のご導入を検討いただきありがとうございます。

TAKETINは、弊社が運用管理するサーバー機器に、弊社が開発しているソフトウェアをインストールし、インターネットを介してお客様にご利用いただくサービス(Software as a Service)になります。

導入が簡単で、インターネットに繋がる環境さえあれば、いつでもどこでも利用いただくことができる便利なサービスとなっています。

弊社では、TAKETINをお客様に安心してご利用いただくために、様々なセキュリティ対策を施しています。

本書では、本書改定日時点でのセキュリティ対策内容についてご説明いたしております。

## TAKETIN(タケチン)が機能として持つセキュリティ対策

TAKETINに実装されているセキュリティ対策機能について説明します。

### パスワードのハッシュ化

お客様(ユーザー)及び管理ユーザーに発行されるパスワードはハッシュ化され、復号できない状態で保存されています。万一データが外部に持ち出されたとしても利用することができません。

### ログインIDとパスワードによるユーザー認証

お客様(ユーザー)毎に、パスワードが発行されログインをするときにはIDとパスワードの両方が求められるようになっていきます。

### 管理者権限の管理(役割と権限)

TAKETINの管理画面で行う作業を、スタッフ毎に行うことができる作業の権限を追加・変更することができます。

### 管理画面を利用できるIPアドレスの制限

管理画面へアクセス可能な場所(IP)を指定することができるようになっていきます。

### 管理画面URLの変更

ディレクトリ名を、分かりづらい文字列にするという方法で、管理画面へのアクセスを容易にできないようにできます。

## サーバー運用・管理上のセキュリティ対策

TAKETINが設置されているデータセンターにおけるセキュリティ対策や、データバックアップの仕組みなどサーバー運用・管理上のさまざまなセキュリティ対策、データ保全対策についてご説明します。

### 管理水準の高いデータセンター

サーバーを設置しているデータセンターは、下記のとおり十分な災害対策や万全のセキュリティ対策が施されています。

1. 制振・耐震・免震構造の設備とハウジングラック
2. 無停電電源装置(UPS)
3. 非常用発電装置
4. 空調設備
5. 防火設備
6. データセンターへの入退室管理

### RAID構成によるデータ保全

お客様のデータを保存するストレージ(HDDやSSD)は、すべてRAID構成となっており、万一運用中に1台のストレージが故障や破損をしても、システムを止める事なく稼働し続けることができます。

### 通信の安全性

通信のすべてをSSL/TLSを用いてデータ暗号化してあるので、第三者が内容を確認することができません。

### ハードディスクの空き容量の監視

サーバーにおいてハードディスクの空き容量がある一定値より少なくなった場合には、運用管理責任者に通知が行われます。

### サーバーへのアクセス制限

サーバーへアクセス出来るのは、弊社の限られた技術者のみが接続できます。また限定された場所(IP)からのみ接続が可能となっています。

## 弊社におけるセキュリティ対策

TAKETINのソフトウェア開発及び社内におけるセキュリティ対策についてご説明します。

### 国際的なセキュリティ基準に則した運用体制

株式会社TAKETINは、国際規格ISO27001 (ISMS)を取得し、厳格なセキュリティ基準に則して運用をおこなっています。

※ISMSとは、組織が保有する情報にかかわるさまざまなリスクを適切に管理し、組織の価値向上をもたらすための国際規格です。

### 開発に関わる関係者とは機密保持契約

開発に関わる全ての従業員(パートナー含む)と機密保持契約を取り交わしています。

### 安心のバックアップ体制

データベースのデータは毎時間、異なる地域のデータセンターへローカル接続を通じてバックアップされており、万が一システム管理者の操作ミスや、災害によってデータセンター自体が機能不全に陥ったとしてもデータを復元することができる体制を取っています。

## 利用上のお願い

お客様がTAKETINをご利用されるにあたってご注意いただきたい事、お願いしたいことをご説明します。

### ユーザーIDの、パスワードの漏洩防止

ユーザーID、パスワード情報の漏洩には十分にご注意していただくようお願いいたします。

### パスワードの定期的な変更

簡単にパスワードの変更が可能ですので、定期的にパスワード変更を行うようお願いいたします。

### 2段階認証の設定

IDやパスワード入力のほかに、アプリが発行するセキュリティコードの入力などを追加することで、本人以外が不正に情報にアクセスすることを防止する仕組みを設定できますので、ぜひご利用をお勧めいたします。

### データバックアップ

障害が発生し、万が一アクセスできなかつたり、データが完全に破損してしまつたりする場合に備えて、顧客データベースのバックアップをしていただくようお願いいたします。

顧客データや契約データは、管理画面より簡単にCSVダウンロードが可能となっています。

### 万が一に備えての保険加入もご検討ください

情報漏えいの多くはサーバーセキュリティだけでなく、人的要因という報告もありますので、ご心配される場合は「[個人情報取扱事業者保険](#)」へのご加入をご検討ください。

※弊社では取次・あっせん等は行っておりません。